

Random groups are not left-orderable

Damian OrleŃ *

Faculty of Mathematics, Informatics and Mechanics,
University of Warsaw,
Banacha 2, 02-097 Warszawa, Poland

May 10, 2016

Abstract

We prove that random groups in the Gromov density model at any density d are with overwhelming probability either non-left-orderable or trivial. It implies the lack of left-orderability for $d < \frac{1}{2}$.

1 Introduction

We work in the density model for random groups introduced by Gromov.

Definition 1.1 (cf. [5, Section 9.B], [8, Definition 7]). Let F_n be the free group on $n \geq 2$ generators a_1, \dots, a_n . For any integer L let $R_L \subset F_n$ be the set of reduced words of length L in these generators.

Let $d \in (0, 1)$. A *random set of relators at density d , at length L* is a sequence of $\lfloor (2n-1)^{dL} \rfloor$ elements of R_L , picked independently and uniformly at random from all elements of R_L .

A *random group at density d , at length L* is the group G presented by $\langle S | R \rangle$, where $S = \{a_1, \dots, a_n\}$ and R is a random set of relators at density d , at length L .

The relators in R_L are not assumed to be cyclically reduced.

Of particular interest in the study of random groups are the properties occurring *with overwhelming probability*.

Definition 1.2 (cf. [5, Section 9.B], [8, Definition 7]). Let $I \subset \mathbb{N}_+$ be infinite. We say that a property of random sets of relators, or of random groups, occurs *with I -overwhelming probability* (shortly, *w. I -o.p.*) *at density d* if its probability of occurrence tends to 1 as $L \rightarrow \infty$, for $L \in I$ and fixed d . We omit writing “ I –” if $I = \mathbb{N}_+$.

2010 *Mathematics Subject Classification*. Primary 20F65. Secondary 20F60.

Key words and phrases. Gromov random groups, orderable groups.

*damian.orleŃ@students.mimuw.edu.pl

Basic characteristics of the model are given by the following phase transition theorem, due to Gromov.

Theorem 1.3 (cf. [5, Section 9.B], [7, Theorem 2]). *A random group is with overwhelming probability*

- *trivial or $\mathbb{Z}/2\mathbb{Z}$ at density $d > \frac{1}{2}$,*
- *infinite, hyperbolic and torsion-free at density $d < \frac{1}{2}$.*

A number of interesting properties are known to hold for random groups w.o.p. at various densities (see [8, Section I.3]).

In this paper we consider the *left-orderability*.

Definition 1.4. A group G is said to be *left-ordered* by \leq if \leq is a total order on G which is *left-invariant*: for all $g_1, g_2, h \in G$ the condition $g_1 \leq g_2$ implies $hg_1 \leq hg_2$.

Our main result is the following.

Theorem 1.5. *Let $d \in (0, 1)$. A random group in the Gromov density model at density d is w.o.p. either trivial or non-left-orderable.*

In conjunction with Theorem 1.3, this shows non-left-orderability of random groups below the critical density $d = \frac{1}{2}$.

If G is a countable group (e.g. a random group), then G is left-orderable if and only if it admits a faithful action on the real line by orientation-preserving homeomorphisms (see [3, Section 1.1.3]). Theorem 1.5 may be thus treated as a result connected to the Gromov conjecture that a random group should not have any smooth actions on any compact manifolds (cf. [4, Conjecture 4.22]).

As a side note, Theorem 1.5 provides also an alternative way of showing that random groups are not free of rank ≥ 1 at any density, since free groups are left-orderable (cf. [1, Theorem 2.3.1]).

The main idea of our proof is to use the order to explicitly construct a high-density set P of words in F_n , representing strictly positive (in the sense of the order) elements of the given random group $G = \langle S | R \rangle$. It happens that for fixed d , the density of P exceeds $(1 - d)$ for n sufficiently large. By a well-known fact it thus contains w.o.p. a word w from the set R of relators, leading to a contradiction of the corresponding element $\bar{w} \in G$ being both positive and trivial. Finally, we use the approach of [2] to increase the number of generators we work with and obtain the result for all $n \geq 2$.

The whole proof is phrased in the language of the b-automata and the associated groups, as introduced in [2] and follows a very similar framework. Just in the case of fixed d and sufficiently large n one can entirely avoid referring to [2] and provide a bit shorter argument. It consists of considering sets $\mathcal{L}_{\varepsilon, i}$ from the proof of Lemma 3.10, proving they all intersect w.o.p a random set of relators by the usual density argument and then proceeding as in the proof of Proposition 3.9.

This paper is structured as follows. Section 2 deals with the basic properties of the left-ordered groups. In Section 3 we introduce the notion of a b-automaton

and its language and use them to give a proof of Theorem 1.5 for n sufficiently large. In Section 4 we use the concept of the associated groups to generalise it to all $n \geq 2$. In Appendix A we reprove a well-known generalisation of the fact that a random set of relators at density d intersects w.o.p. any fixed set of relators of density d' such that $d + d' > 1$. The more general statement is that their intersection is roughly of density $d + d' - 1$ if $d < \frac{1}{2}$ (cf. [5, Section 9.A]). The assumption on d is not really limiting, in view of Theorem 1.3. It comes from the fact that we define “a random set at density d ” to be a tuple with possible repetitions. If we, however, have $d < \frac{1}{2}$, then there are w.o.p. no such repetitions and the counting is easier.

Acknowledgements

Yago Antolin-Pichel, in private communication, suggested the use of Lemma 2.4, which is the key property of the left-ordered groups used in the proof. Piotr Przytycki suggested the topic of this paper, encouraged and advised the author. I would like to thank both of them.

2 Left orders

Let G be a group left-ordered by \leq . Symbols $<$ and $>$ are the usual shorthands. By e we denote the neutral element of G . The following remarks are easily obtained from Definition 1.4.

Remark 2.1. Any non-empty product of elements strictly greater than e is itself strictly greater than e .

Remark 2.2. For every $g \in G \setminus \{e\}$ one can choose a sign $\varepsilon \in \{-1, 1\}$ such that $g^\varepsilon > e$.

Those two imply quickly the following.

Corollary 2.3. G is torsion-free.

Proof. Take any $g \in G \setminus \{e\}$. By Remark 2.2, we can choose $\varepsilon \in \{-1, 1\}$ such that $g^\varepsilon > e$. Remark 2.1 implies now that for every $n \geq 1$ we have $g^{n\varepsilon} > e$, so g is not a torsion element. \square

Moreover, by combining Remarks 2.1 and 2.2, we obtain Lemma 2.4, which will be used in a moment to construct high-density sets of words representing non-trivial elements. It was suggested by Yago Antonin-Pichel.

Lemma 2.4. For every choice of non-trivial $g_1, \dots, g_n \in G$ there exists a sequence of signs $\varepsilon_1, \dots, \varepsilon_n \in \{-1, 1\}$ for which every non-empty product (possibly with repetitions) of elements of form $g_i^{\varepsilon_i}$ is non-trivial.

Proof. Choose $(\varepsilon_i)_{i=1}^n$ for which $g_i^{\varepsilon_i} > e$ for $i = 1, \dots, n$. \square

Lemma 2.4 is in fact equivalent to G being left-orderable, but we will only need the implication we proved (cf. [1, Theorem 7.1.1]).

3 Random groups with large number of generators

We begin by reproducing terminology and useful observations of [2, Section 2]. By S we denote a finite set, called the *alphabet*. We define S^{-1} to be the set of formal inverses to the elements of S , and denote $S^\pm = S \cup S^{-1}$. Elements of S^\pm are called the *letters*. By *word over an alphabet S* we mean a finite sequence of *letters*. We denote $S = \{a_1, \dots, a_n\}$, hence $n = |S|$. S is to be interpreted as the set of generators of F_n .

Definition 3.1 (cf. [2, Definition 2.1]). A *basic automaton* (shortly a *b-automaton*) over an alphabet S with transition data $\{\sigma_s\}$ is a pair $(S, \{\sigma_s\})$, where $\{\sigma_s\}_{s \in \{\emptyset\} \cup S^\pm}$ is a family of subsets of S^\pm .

The *language* of a b-automaton with transition data $\{\sigma_s\}$ is the set of all non-empty words over S beginning with a letter in σ_\emptyset and such that for any two consecutive letters ss' we have $s' \in \sigma_s$.

We say that a b-automaton is λ -large, for some $\lambda \in (0, 1)$, if $\sigma_\emptyset \neq \emptyset$ and for each $s \in S^\pm$ we have $|\sigma_s| \geq \lambda 2n$.

Remark 3.2 (cf. [2, Remark 2.2(i)]). There are exactly $2^{2n(2n+1)}$ many b-automata over a fixed alphabet S of size n .

Remark 3.3 (cf. [2, Remark 2.2(ii)]). If a b-automaton is λ -large, then its language contains at least $\lceil \lambda 2n \rceil^{L-1}$ words of length L and at least $(\lceil \lambda 2n \rceil - 1)^{L-1}$ reduced words of length L .

Definition 3.4 (cf. [2, Definition 2.3]). Let $I \subset \mathbb{N}_+$ be infinite and let \mathcal{L} be a set of reduced words over an alphabet S , containing for all but finitely many $L \in I$ at least ck^L words of length L , where $c > 0, k > 1$. Then we say that the *I -growth rate of \mathcal{L} is at least k* . Similarly, if $k > k'$, then we say that the *I -growth rate of \mathcal{L} is greater than k'* .

It is convenient to extend the notion of density from Definition 1.1 in the following way.

Definition 3.5. Let $I \subset \mathbb{N}_+$ be infinite and let \mathcal{L} be a set of reduced words over an alphabet S , containing for all but finitely many $L \in I$ at least $c(2n-1)^{dL}$ words of length L , where $c > 0, d \in (0, 1)$. Then we say that the *I -density of \mathcal{L} is at least d* .

Notions of density d and growth rate k of the set \mathcal{L} are easily seen to be strictly related by $k = (2n-1)^d$, i.e. for such k, d , with $d \in (0, 1)$, the set \mathcal{L} has I -growth rate at least k if and only if it has I -density at least d .

The following is a well known fact in random groups. We reprove it in a stronger form in Appendix A.

Proposition 3.6 (cf. [5, Section 9.A]). *Let $I \subset \mathbb{N}_+$ be infinite. Suppose $d, d' \in (0, 1)$ are such that $d + d' > 1$ and $R_f \subset F_n$ is a fixed set of relators in some fixed number n of generators, of I -density at least d' . Then w. I-o.p. a random set R of relators at density d intersects R_f .*

From this we get

Lemma 3.7 (cf. [2, Lemma 2.4]). *Let $I \subset \mathbb{N}_+$ be infinite and let \mathcal{L} be a set of reduced words over the alphabet S , of I -growth rate greater than $(2n-1)^{1-d}$, for some $d \in (0, 1)$. Then w. I-o.p. a random set of relators at density d intersects \mathcal{L} .*

We will be interested in the following consequence.

Corollary 3.8 (cf. [2, Corollary 2.5]). *For given $\lambda, d \in (0, 1)$, if n is sufficiently large, then w.o.p. a random set of relators at density d intersects the languages of all λ -large b -automata over the alphabet S .*

Proof. As the number of the b -automata over S is finite and depends only on n (by Remark 3.2), we just need to show that there exists n_0 , for which if $n \geq n_0$, then the conclusion holds for the language \mathcal{L} of every single λ -large b -automaton. By Remark 3.3, the \mathbb{N}_+ -growth rate of the set of the reduced words in \mathcal{L} is at least $\lceil \lambda 2n \rceil - 1$, hence, by Lemma 3.7, the following inequality suffices.

$$\lceil \lambda 2n \rceil - 1 > (2n - 1)^{1-d}$$

As $d \in (0, 1)$, this inequality holds for n large enough. \square

For a group G with presentation $G = \langle S | R \rangle$ and a word w over the alphabet S , we will denote by \overline{w} the corresponding element of G .

To obtain Theorem 1.5 for n sufficiently large, we just need the following.

Proposition 3.9. *Let G be a group with presentation $G = \langle S | R \rangle$ such that R intersects the languages of all $\frac{1}{2}$ -large b -automata over the alphabet $S = \{a_1, \dots, a_n\}$. Then G is either trivial or non-left-orderable.*

In order to prove Proposition 3.9, we use the following lemma, which is our main step towards the exploiting the hypothetical left-orderability of random groups.

Lemma 3.10. *Let R be a set of words over the alphabet S . Assume R intersects the languages of all $\frac{1}{2}$ -large b -automata over S . Then for every choice of signs $\varepsilon = (\varepsilon_1, \dots, \varepsilon_n) \in \{-1, 1\}^n$ and a number $i \in \{1, \dots, n\}$, there exists a non-empty reduced word $w \in R$, consisting only of letters from the set $\{a_1^{\varepsilon_1}, a_2^{\varepsilon_2}, \dots, a_n^{\varepsilon_n}\}$, with at least one occurrence of $a_i^{\varepsilon_i}$.*

Proof of Lemma 3.10. Consider a b -automaton $\mathbb{A}_{\varepsilon, i}$ over S with transition data $\sigma_\emptyset = \{a_i^{\varepsilon_i}\}$ and $\sigma_s = \{a_1^{\varepsilon_1}, \dots, a_n^{\varepsilon_n}\}$ for every $s \in S^\pm$. Every word in its language $\mathcal{L}_{\varepsilon, i}$ is reduced. $\mathbb{A}_{\varepsilon, i}$ is $\frac{1}{2}$ -large, hence there exists some $w \in \mathcal{L}_{\varepsilon, i} \cap R$. The word w starts with $a_i^{\varepsilon_i}$ and it satisfies the conditions we imposed. \square

Proof of Proposition 3.9. Suppose G is left-orderable, but non-trivial.

Let $a_{i_1}, a_{i_2}, \dots, a_{i_m}$ be all those elements $a_j \in S$, such that $\overline{a_j} \in G$ is non-trivial. There must be at least one, since G is generated by elements $\overline{a_j}$. According to Lemma 2.4, we can find signs $\varepsilon_{i_1}, \dots, \varepsilon_{i_m} \in \{-1, 1\}$, such that every non-empty word consisting of letters from $\{a_{i_1}^{\varepsilon_{i_1}}, \dots, a_{i_m}^{\varepsilon_{i_m}}\}$ represents a non-trivial element of G . Note that those words are always reduced.

Now for $j \in \{1, \dots, n\} \setminus \{i_1, \dots, i_m\}$ choose $\varepsilon_j \in \{-1, 1\}$ in arbitrary way. We have thus defined a sequence $\varepsilon_1, \dots, \varepsilon_n \in \{-1, 1\}$. By Lemma 3.10 applied to this sequence and $i = i_1$, we obtain a word w which lies in R , so it represents the trivial element of G , and consists of letters of form $a_j^{\varepsilon_j}$ with at least one occurrence of $a_{i_1}^{\varepsilon_{i_1}}$. As $a_j^{\varepsilon_j}$ for $j \notin \{i_1, \dots, i_m\}$ represent the trivial element, we can remove all occurrences of such letters from w and obtain that way a word w_1 , still representing the trivial element and consisting only of letters of form $a_{i_j}^{\varepsilon_{i_j}}$. w_1 is, however, non-empty because of at least one occurrence of $a_{i_1}^{\varepsilon_{i_1}}$. We arrive thus at a contradiction with the earlier definition of signs $\varepsilon_{i_1}, \dots, \varepsilon_{i_m}$. \square

For fixed $d \in (0, 1)$ and $\lambda = \frac{1}{2}$ there is n_0 such that the conclusion of Corollary 3.8 holds for all $n \geq n_0$. For such n Theorem 1.5 is now almost immediate.

Proof of Theorem 1.5 for $n \geq n_0$. A random group G at density d is w.o.p. presented by $\langle S | R \rangle$, where R intersects the languages of all $\frac{1}{2}$ -large b-automata over S , so, by Proposition 3.9, it is either trivial or non-left-orderable. \square

4 Increasing the number of generators

We now generalise our partial proof of Theorem 1.5 to arbitrary values of $n \geq 2$. We follow closely the ideas of [2, Section 3].

We fix $n \geq 2$ and $d \in (0, 1)$. We furthermore fix B to be a natural number that is sufficiently large with respect to n and d in a way we will specify later.

As before, we denote by S the set of generators $\{a_1, \dots, a_n\}$. Let $\tilde{S} \subset F_n$ denote the set of reduced words of length B over the alphabet S . The involution on \tilde{S} mapping each word to its inverse does not have fixed points. Thus we can partition \tilde{S} into \hat{S} and \hat{S}^{-1} . We introduce the notation $\hat{S}^\pm = \hat{S} \cup \hat{S}^{-1}$ in place of \tilde{S} . Let \hat{n} be the number $|\hat{S}| = n(2n-1)^{B-1}$.

Furthermore, for $0 \leq P < B$ let $I_P \subset \mathbb{N}_+$ denote the set of those L that can be written as $L = B\hat{L} + P$ with $\hat{L} > 0$.

Definition 4.1 ([2, Definition 3.1]). Let r be a word of length $L \in I_0$ over the alphabet S . Divide the word r into \hat{L} blocks of length B . This determines a new word \hat{r} of length \hat{L} over the alphabet \hat{S} , which we call the word *associated* to r .

Definition 4.2 ([2, Definition 3.2]). Given a set R of reduced relators over S of equal length $L \in I_P$, we define the *associated group* \hat{G} in the following way.

If $P = 0$, then we consider the set \hat{R} of relators associated to relators in R . We define \hat{G} to be the group $\langle \hat{S} | \hat{R} \rangle$.

If $1 \leq P < B$, then we do the following construction. Suppose that $r_1, r_2 \in R$ are two relators of length L over S , satisfying $r_1 = q_1 v^{-1}$ and $r_2 = v q_2$ (we assume q_1, q_2, v to be reduced and that there are no reductions between q_1 and v^{-1} or between v and q_2), for some word v over S of length P . We then obtain a (possibly non-reduced) word $q_1 q_2$ over S , of length $2B\hat{L}$, with the property that $\overline{q_1 q_2} = e$ in $G = \langle S | R \rangle$. To this word we can associate, as before, a relator over \hat{S} ,

of length $2\hat{L}$ (possibly non-reduced), which we denote by $\hat{r}(r_1, r_2)$. We denote by \hat{R} the set of all $\hat{r}(r_1, r_2)$ as above and we define $\hat{G} = \langle \hat{S} | \hat{R} \rangle$.

The main intuition here is that \hat{R} obtained from a random set R of relators over S , at density d , at length $L \in I_0$ is very similar to a random set of relators over \hat{S} , at the same density d , at length $\frac{L}{B}$ (see [2, Section 3]).

By increasing B , the number \hat{n} can be made arbitrarily large. We can thus have \hat{n} large enough to obtain the conclusion of Corollary 3.8 for intersections of languages of $\frac{1}{2}$ -large b -automata over \hat{S} with random sets of relators at density d . We then use the following analogue of Proposition 3.9.

Proposition 4.3. *Suppose that \hat{R} , obtained as in Definition 4.2 from R being a set of reduced relators of the same length, intersects languages of all $\frac{1}{2}$ -large b -automata over \hat{S} . Then $G = \langle S | R \rangle$ is either trivial or non-left-orderable.*

Proof. Suppose G is non-trivial and left-orderable. The construction of \hat{G} was performed in such a way, that by expanding elements of \hat{S} into words over S we get a natural epimorphism $\phi : \hat{G} \rightarrow H$, where H is the subgroup of G generated by the reduced words of length B over S .

We note that $H \subset G$ is of finite index, since every element $g \in G$ is of form $g = \bar{w}$ for some reduced word w over S and we may write $w = uv$ with u of length at most B and v of length divisible by B . We have thus $\bar{v} \in H$, hence $g \in \bar{u}H$ and the index $[G : H]$ is not greater than the number of possible values of \bar{u} , which is finite.

Moreover, H is non-trivial, because otherwise G would be finite and non-trivial, hence not torsion-free, contradicting left-orderability (by Corollary 2.3).

Denote elements of \hat{G} , represented by single letters from \hat{S} , by $b_1, \dots, b_{\hat{n}}$. They generate \hat{G} , so H is generated by $\phi(b_1), \dots, \phi(b_{\hat{n}})$, not all of them being trivial. Let $\phi(b_{i_1}), \dots, \phi(b_{i_m})$ be all non-trivial elements of form $\phi(b_j)$. The subgroup H is left-orderable, so, by Lemma 2.4, there exist signs $\varepsilon_{i_1}, \dots, \varepsilon_{i_m} \in \{-1, 1\}$, such that every non-empty product of elements of form $\phi(b_{i_j})^{\varepsilon_{i_j}}$ is non-trivial. In arbitrary way we choose $\varepsilon_i \in \{-1, 1\}$ for $i \in \{1, \dots, \hat{n}\} \setminus \{i_1, \dots, i_m\}$.

Fix $i = i_1$. For this index i and the set \hat{R} of words over \hat{S} we apply Lemma 3.10 to conclude that there exists a product of elements of form $b_j^{\varepsilon_j}$, with at least one occurrence of $b_{i_1}^{\varepsilon_{i_1}}$, which evaluates to the trivial element in $\hat{G} = \langle \hat{S} | \hat{R} \rangle$.

By evaluating ϕ on this product, we get a product of elements of form $\phi(b_j)^{\varepsilon_j}$, with at least one occurrence of $\phi(b_{i_1})^{\varepsilon_{i_1}}$, which evaluates to the trivial element in H . Finally, by leaving the non-trivial factors only, we get a non-empty product of elements of form $\phi(b_{i_j})^{\varepsilon_{i_j}}$, evaluating to the trivial element, which is a contradiction with the definition of signs $\varepsilon_{i_1}, \dots, \varepsilon_{i_m}$. □

The last element of the proof of Theorem 1.5 is the following.

Lemma 4.4 ([2, Section 3]). *If B is sufficiently large, then, in Gromov density model with n generators, a random set R of relators at density d has w.o.p the property, that the set \hat{R} , obtained from R as in Definition 4.2, intersects languages of all $\frac{1}{2}$ -large b -automata over \hat{S} .*

Assuming Lemma 4.4, the proof of Theorem 1.5 is straightforward.

Proof of Theorem 1.5. Let B be sufficiently large for the conclusion of Lemma 4.4 to hold. Then, by the combination of Proposition 4.3 and Lemma 4.4, a random group $G = \langle S | R \rangle$ in Gromov density model is w.o.p. either non-left-orderable or trivial. \square

The proof of Lemma 4.4 (in slightly stronger form) is given in [2, Section 3] in the first 5 lines of the proof of [2, Theorem 1.5]. The hypothesis of [2, Proposition 2.6] for group $\hat{G} = \langle \hat{S} | \hat{R} \rangle$, obtained from a random group $G = \langle S | R \rangle$, is checked there, which amounts to proving that \hat{R} , obtained from a random set R of relators in Gromov model, intersects languages of all $\frac{1}{3}$ -large b -automata over \hat{S} . It remains to note that all $\frac{1}{2}$ -large b -automata are, in particular, $\frac{1}{3}$ -large.

In the rest of this section we reproduce this proof to make the exposition as self-contained as possible.

In order to prove Lemma 4.4, we develop a few technical results.

The following suffices to prove the conclusion of Lemma 4.4 w. I_0 -o.p.

Lemma 4.5 ([2, Lemma 3.4]). *Let \mathbb{A} be a λ -large b -automaton over \hat{S} . Denote by $\mathcal{L}_{\mathbb{A}}$ the set of reduced words over S , of length divisible by B , whose associated words lie in the language of \mathbb{A} . Assume that $\lambda' = \lambda - \frac{1}{2n} > 0$. Then the I_0 -growth rate of $\mathcal{L}_{\mathbb{A}}$ is at least $\sqrt[B]{\lambda'}(2n - 1)$.*

Proof. Let $\{\sigma_{\hat{s}}\}$ denote the transition data of \mathbb{A} . For any $\hat{s} \in \hat{S}^{\pm}$, let $\rho_{\hat{s}} \subset \hat{S}^{\pm}$ be the set of \hat{s}' such that the first letter of \hat{s}' interpreted as a word over the alphabet S is the inverse of the last letter of \hat{s} as a word over S . We see that $|\rho_{\hat{s}}| = \frac{1}{2n}2\hat{n}$.

Let \mathbb{A}^{red} be the b -automaton over \hat{S} with transition data $\sigma_{\emptyset}^{\text{red}} = \sigma_{\emptyset}$ and $\sigma_{\hat{s}}^{\text{red}} = \sigma_{\hat{s}} \setminus \rho_{\hat{s}}$, for $\hat{s} \in \hat{S}^{\pm}$. We have thus $|\sigma_{\hat{s}}^{\text{red}}| \geq |\sigma_{\hat{s}}| - |\rho_{\hat{s}}| \geq \lambda 2\hat{n} - \frac{1}{2n}2\hat{n} = \lambda' 2\hat{n}$. Hence \mathbb{A}^{red} is λ' -large and its language contains at least $\lceil \lambda' 2\hat{n} \rceil^{\hat{L}-1}$ words of length \hat{L} , by Remark 3.3.

The language of \mathbb{A}^{red} is a subset of the language of \mathbb{A} and consists only of such words w over \hat{S} , that if we substitute each letter $\hat{s} \in w$ with the corresponding word over S , we obtain a reduced word over S , of length $B\hat{L}$, if \hat{L} is the length of w .

It means that the number of reduced words of length $L = B\hat{L}$ over S , whose associated words lie in the language of \mathbb{A} , is at least

$$(\lceil \lambda' 2\hat{n} \rceil)^{\hat{L}-1} \geq (\lambda' 2\hat{n})^{\frac{L}{B}-1} \geq c \left(\sqrt[B]{\lambda' 2\hat{n}} \right)^L$$

for some $c > 0$, independent of L . The I_0 -growth rate of $\mathcal{L}_{\mathbb{A}}$ is thus at least $\sqrt[B]{\lambda' 2\hat{n}}$. To finish the proof it remains to notice that

$$\sqrt[B]{\lambda' 2\hat{n}} > \sqrt[B]{\lambda'(2n - 1)^B} = \sqrt[B]{\lambda'}(2n - 1).$$

\square

We deduce the following corollaries from Lemma 4.5 in order to deal with the case of relators of length in I_P , for $1 \leq P < B$.

Let us consider the setting of Lemma 4.5. Let $\mathcal{P}_{\mathbb{A}}^P$ (the “prefix set”) denote the set of reduced words w over S , whose length L lies in I_P , such that the length $B\hat{L} = L - P$ prefix of w lies in $\mathcal{L}_{\mathbb{A}}$. Every word in $\mathcal{L}_{\mathbb{A}}$ extends to at least one word in $\mathcal{P}_{\mathbb{A}}^P$ by addition of P letters on its right end, so from Lemma 4.5 we obtain the following.

Corollary 4.6 ([2, Corollary 3.5]). *The I_P -growth rate of $\mathcal{P}_{\mathbb{A}}^P$ is at least $\sqrt[B]{\lambda'}(2n - 1)$.*

Let us consider the set of reduced words of length B over S , which begin with s^{-1} , for a given $s \in S^{\pm}$. We interpret it as a subset ρ^s of \hat{S}^{\pm} . For any $\hat{s} \in \hat{S}^{\pm}$, let $\mathbb{A}^{\hat{s},s}$ be the b-automaton over \hat{S} with transition data equal to the transition data of \mathbb{A} with the exception that we substitute σ_{\emptyset} with $\sigma_{\hat{s}} \setminus \rho^s$. This set is nonempty since $|\rho^s| = \frac{1}{2n}2\hat{n}$ and we assumed both $|\sigma_{\hat{s}}| \geq \lambda 2\hat{n}$ and $\lambda > \frac{1}{2n}$. Hence $\mathbb{A}^{\hat{s},s}$ is λ -large.

Let v be a reduced word of length P over S , ending with a letter s . For any $\hat{s} \in \hat{S}^{\pm}$, let $\mathcal{S}_{\mathbb{A}}^{\hat{s},v}$ (the “suffix set”) denote the set of words w over S , of length $L \in I_P$, such that the length P prefix of w equals v , and the length $B\hat{L} = L - P$ suffix of w lies in $\mathcal{L}_{\mathbb{A}^{\hat{s},s}}$. Every word in $\mathcal{S}_{\mathbb{A}}^{\hat{s},v}$ is reduced, because all words in the language of $\mathbb{A}^{\hat{s},s}$ start with a letter outside of ρ^s , so all words in $\mathcal{L}_{\mathbb{A}^{\hat{s},s}}$ start with a letter different from s^{-1} .

Now, by applying Lemma 4.5 to $\mathbb{A}^{\hat{s},s}$, we obtain the last corollary needed.

Corollary 4.7 ([2, Corollary 3.6]). *The I_P -growth rate of $\mathcal{S}_{\mathbb{A}}^{\hat{s},v}$ is at least $\sqrt[B]{\lambda'}(2n - 1)$.*

Now we can finally prove Lemma 4.4.

Proof of Lemma 4.4. Let B be large enough for the inequality $\sqrt[B]{4} < (2n - 1)^d$ to hold. Let R denote a random set of relators at density d . There are finitely many sets of form I_P and finitely many b-automata over \hat{S} , so we just need to show that for every $0 \leq P < B$ and every $\frac{1}{2}$ -large b-automaton \mathbb{A} over \hat{S} , the set \hat{R} intersects the language of \mathbb{A} w. I_P -o.p.

Consider first the case where $P = 0$. By Lemma 4.4, the I_0 -growth rate of $\mathcal{L}_{\mathbb{A}}$ is at least $\sqrt[B]{\lambda'}(2n - 1)$, where

$$\lambda' = \frac{1}{2} - \frac{1}{2n} \geq \frac{1}{4}$$

as $n \geq 2$, so the I_0 -growth rate of $\mathcal{L}_{\mathbb{A}}$ is at least $\frac{2n-1}{\sqrt[B]{4}} > (2n - 1)^{1-d}$. Hence, by Lemma 3.7, the set R intersects $\mathcal{L}_{\mathbb{A}}$ w. I_0 -o.p., so \hat{R} intersects the language of \mathbb{A} w. I_0 -o.p.

In the remaining case, we have $1 \leq P < B$. The number of the sets of form $\mathcal{S}_{\mathbb{A}}^{\hat{s},v}$ is finite and independent of L , so by corollaries 4.6 and 4.7 and by Lemma 3.7, we obtain, in the same way as in the previous case, that w. I_P -o.p. the set R intersects the set $\mathcal{P}_{\mathbb{A}}^P$ and every set of form $\mathcal{S}_{\mathbb{A}}^{\hat{s},v}$.

When it happens, take $r_1 \in R \cap \mathcal{P}_{\mathbb{A}}^P$. Denote by v^{-1} the word consisting of last P letters of r_1 and by $\hat{s} \in \hat{S}^{\pm}$ the letter associated to the length B block

appearing before v^{-1} in r_1 . Denote by s the last letter of v . Now we can take $r_2 \in R \cap \mathcal{S}_{\mathbb{A}}^{\hat{s},v}$. There are reduced words $q_1 \in \mathcal{L}_{\mathbb{A}}, q_2 \in \mathcal{L}_{\mathbb{A}^{\hat{s},s}}$, such that $r_1 = q_1 v^{-1}$ and $r_2 = v q_2$ (as in Definition 4.2). Denote by \hat{q}_1, \hat{q}_2 the words associated to q_1, q_2 . The words \hat{q}_1 and \hat{q}_2 , lie, respectively, in the languages of \mathbb{A} and $\mathbb{A}^{\hat{s},s}$. Moreover, \hat{q}_1 finishes with \hat{s} , so by definition of $\mathbb{A}^{\hat{s},s}$, the word $\hat{q}_1 \hat{q}_2$ belongs to the language of \mathbb{A} , so the relator $\hat{r}(r_1, r_2) = \hat{q}_1 \hat{q}_2$ belongs to both \hat{R} and the language of \mathbb{A} . \square

A Intersections of high-density sets

From now on, by $I \subset \mathbb{N}_+$ we denote a fixed infinite subset and all limits with $L \rightarrow \infty$ are taken over $L \in I$. The main result of this appendix is the following.

Proposition A.1. *Suppose that for each $L \in I$ we have a set R_L of size $c_L > 0$ with $a_L > 0$ elements distinguished. For fixed L we pick uniformly and independently at random entries of a b_L -tuple ($b_L > 0$) from R_L and obtain this way a random variable D_L equal to the number of the entries of the resulting tuple being distinguished. Assume that $\frac{a_L b_L}{c_L} \rightarrow \infty$ as $L \rightarrow \infty$. Then for every $\varepsilon > 0$ the following holds*

$$\lim_{L \rightarrow \infty} \mathbb{P} \left((1 - \varepsilon) \frac{a_L b_L}{c_L} \leq D_L \leq (1 + \varepsilon) \frac{a_L b_L}{c_L} \right) = 1. \quad (1)$$

Before proving Proposition A.1, let us use it to give a proof of Proposition 3.6 and its generalisation.

Proof of Proposition 3.6. Let c_L , for $L \in I$, denote the number of all reduced relators of length L over S , i.e. $c_L = |R_L| = 2n(2n-1)^{L-1}$. Moreover, let $a_L = |R_f \cap R_L|$ be the number of relators of length L we distinguish by wanting them to be selected in the random tuple. Let $b_L = \lfloor (2n-1)^{dL} \rfloor$. We assume $a_L \geq C(2n-1)^{d'L}$ for $L \in I$ sufficiently large and some $C > 0$. At length L , R is a tuple of b_L elements, chosen uniformly and independently at random from R_L . Let D_L be as in Proposition A.1. Note that $\frac{a_L b_L}{c_L} \rightarrow \infty$ as $L \rightarrow \infty$, since $d + d' > 1$. We may thus apply Proposition A.1 for any $\varepsilon > 0$ to see that a random set R of relators at density d , at length L has w. I -o.p. at least $D_L \geq (1 - \varepsilon) \frac{a_L b_L}{c_L} \geq K(2n-1)^{(d+d'-1)L}$ entries from R_f , for some $K > 0$. For L sufficiently large it clearly implies that R and R_f intersect. \square

If we moreover assume that $d < \frac{1}{2}$ and R_f is roughly (not just at least) of density d' , then we can prove that the intersection is roughly of density $d + d' - 1$.

Proposition A.2. *Suppose $d, d' \in (0, 1)$ are such that $d + d' > 1$ and $d < \frac{1}{2}$. Let $R_f \subset F_n$ be a fixed set of relators in some fixed number n of generators, such that for some $C_1, C_2 > 0$ the inequalities*

$$C_1(2n-1)^{d'L} \leq |R_f \cap R_L| \leq C_2(2n-1)^{d'L}$$

hold for all sufficiently large $L \in I$.

Then for some $K_1, K_2 > 0$ a random set R of relators at density d , at length L satisfies w. I-o.p. the inequalities

$$K_1(2n-1)^{(d+d'-1)L} \leq |R_f \cap R| \leq K_2(2n-1)^{(d+d'-1)L},$$

where $|R_f \cap R|$ denotes the number of distinct entries of R , belonging to R_f .

Proof. We use the notation from the proof of Proposition 3.6. Analogously to that proof, for some $K_1, K_2 > 0$ we obtain

$$K_1(2n-1)^{(d+d'-1)L} \leq D_L \leq K_2(2n-1)^{(d+d'-1)L}, \quad (2)$$

occurring w. I-o.p.

Since $d < \frac{1}{2}$, we have $\frac{b_L^2}{c_L} \rightarrow 0$ as $L \rightarrow \infty$.

Let us estimate the probability q_L that in the experiment defining D_L all elements of the obtained b_L -tuple are pairwise distinct. It is the same as the probability that every element of the tuple is different from the elements having smaller indices (we assume some fixed order on a tuple), so

$$q_L = 1 \left(1 - \frac{1}{c_L}\right) \left(1 - \frac{2}{c_L}\right) \dots \left(1 - \frac{b_L-1}{c_L}\right) \geq \left(1 - \frac{b_L-1}{c_L}\right)^{b_L}.$$

For $L \in I$ sufficiently large we have $\frac{b_L^2}{c_L} < 1$, so $b_L \leq b_L^2 < c_L$ and the number $x_L = -\frac{b_L-1}{c_L}$ satisfies $x_L \geq -1$. It means that we can use Bernoulli's inequality to obtain

$$q_L \geq \left(1 + \left(-\frac{b_L-1}{c_L}\right)\right)^{b_L} \geq 1 - b_L \frac{b_L-1}{c_L}.$$

Obviously, $b_L \frac{b_L-1}{c_L} \rightarrow 0$ as $L \rightarrow \infty$, because $\frac{b_L^2}{c_L} \rightarrow 0$ as $L \rightarrow \infty$. It follows that $q_L \rightarrow 1$ as $L \rightarrow \infty$, so w. I-o.p. the number D_L is the number of distinct entries of R belonging to R_f , which combined with (2) concludes the proof. \square

For the proof of Proposition A.1 we will apply the following bound known as the Chebyshev's inequality.

Lemma A.3 ([6, Lemma 3.1]). *If ξ is a random variable with $\mathbb{E}\xi^2 < \infty$, then for every $\alpha > 0$*

$$\mathbb{P}(|\xi - \mathbb{E}\xi| \geq \alpha) \leq \frac{\text{Var } \xi}{\alpha^2}.$$

Proof of Proposition A.1. Fix $L \in I$. For $i = 1, \dots, b_L$ denote by $X_i^{(L)}$ the random variable equal to 1, if i -th element of the considered random tuple is distinguished, and equal to 0, otherwise.

Variables $(X_i^{(L)})_i$ are independent and $\mathbb{P}(X_i^{(L)} = 1) = \frac{a_L}{c_L} = 1 - \mathbb{P}(X_i^{(L)} = 0)$, so $\mathbb{E}X_i^{(L)} = \frac{a_L}{c_L}$. Next we check that $\text{Var } X_i^{(L)} = \frac{a_L}{c_L}(1 - \frac{a_L}{c_L})$. Since $D_L = \sum_{i=1}^{b_L} X_i^{(L)}$,

we have $\mathbb{E}D_L = \frac{a_L b_L}{c_L}$ and $\text{Var } D_L = \frac{a_L b_L}{c_L} (1 - \frac{a_L}{c_L})$. Fix $\varepsilon > 0$. Now we apply Lemma A.3 for $\xi = D_L$ and $\alpha = \varepsilon \mathbb{E}D_L$, obtaining

$$\begin{aligned} \mathbb{P} \left(\left| D_L - \frac{a_L b_L}{c_L} \right| \geq \varepsilon \frac{a_L b_L}{c_L} \right) &= \mathbb{P} (|D_L - \mathbb{E}D_L| \geq \varepsilon \mathbb{E}D_L) \\ &\leq \frac{\text{Var } D_L}{(\varepsilon \mathbb{E}D_L)^2} = \frac{1 - \frac{a_L}{c_L}}{\varepsilon^2 \frac{a_L b_L}{c_L}} \leq \frac{1}{\varepsilon^2 \frac{a_L b_L}{c_L}} \rightarrow 0 \end{aligned}$$

as $L \rightarrow \infty$, since we assumed that $\frac{a_L b_L}{c_L} \rightarrow \infty$. □

References

- [1] Botto Mura, R., Rhemtulla, A.: *Orderable groups*. Lecture Notes in Pure and Applied Mathematics, Vol. **27**. Marcel Dekker, New York-Basel (1977)
- [2] Dahmani, F., Guirardel, V., Przytycki, P.: *Random groups do not split*. In: Mathematische Annalen **349**(3), pp. 657-673 (2011)
- [3] Deroin, B., Navas, A., Rivas, C.: *Groups, orders, and dynamics*. arXiv:1408.5805 [math.GR] (2014)
- [4] Furman, A.: *A survey of measured group theory*. In: Geometry, Rigidity, and Group Actions. Chicago Lectures in Mathematics Series, pp. 296-374, The University of Chicago Press, Chicago (2011)
- [5] Gromov, M.: *Asymptotic invariants of infinite groups*. In: Geometric Group Theory, vol. 2 (Sussex, 1991). London Mathematical Society Lecture Note Series, vol. 182, pp. 1-295. Cambridge University Press, Cambridge (1993)
- [6] Kallenberg, O.: *Foundations of Modern Probability*, Springer Series in Statistics. Probability and its applications (1997)
- [7] Ollivier, Y.: *Sharp phase transition theorems for hyperbolicity of random groups*. In: Geom. Funct. Anal. **14**(3), 595-679 (2004)
- [8] Ollivier, Y.: *A January 2005 invitation to random groups*. In: Ensaio Matemáticos (Mathematical Surveys), vol. 10. Sociedade Brasileira de Matemática, Rio de Janeiro (2005)